FUJITSU

# Fujitsu
# Enterprise Postgres 16
## Advanced Edition with Cryptographic Module

# Read First

Linux

J2UL-2969-01ENZ0(00)
July 2024

# Preface

## Purpose of this document

This document provides an overview of the Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module, its features, and how to install it.

Read this before using Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

## Intended readers

This document is intended for use with Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

### Export restrictions

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

### Issue date and version

Edition 1.0: July 2024

### Copyright

# Contents

# Chapter 1 Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module Basics

Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module is a product that is configured to use algorithms that are approved by the security requirements for cryptographic modules (FIPS 140), one of the FIPS (Federal Information Processing Standard) standards.

The Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module provides the same feature as the Fujitsu Enterprise Postgres Advanced Edition.

This chapter describes the differences between Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module and Fujitsu Enterprise Postgres Advanced Edition regarding the features, operating environment, installation, setup, and application development.

## 1.1 Feature Differences from Fujitsu Enterprise Postgres Advanced Edition

### Encryption features

If you use a cryptographic module provided by Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module, you cannot use "Algorithms not approved for FIPS 140", so the following cryptographic functionality differences exist:

- Saving Passwords in md5 format on the server
  Use the default scram-sha-256.
- Some algorithms used to connect and authenticate using SSL
  Not only are they not available as encryption algorithms for communication paths, but they are also not available as signature algorithms for certificates, encryption algorithms for encrypting and storing private keys, and so on.
- The following are not available
  - md5 in SQL functions
  - Some algorithms of the extension module pgcrypto
  - Some functions of the extension module uuid-ossp

Algorithms not approved for FIPS 140

| Classification | Details |
|---|---|
| Algorithms | BF, CAST, DES, DESX, IDEA, RC2, RC4, RC5, SEED, ARIA, CAMELLIA, SM4 |
| Digest | MD2, MD4, MDC2, DES, RIPEMD-160, WHIRLPOOL,BLAKE2, SM3, MD5, MD5-SHA1 |
| MAC | BLAKE2, CMAC, KMAC, POLY1305, SIPHASH |
| KDF | KBKDF, KRB5KDF, SCRYPT, X942KDF, X963KDF |
| Asymmetric keys | RSA-PSS, RSA-OAEP, SM2 |
| Asymmetric encryption | RSAES-OAEP |

### Application development

JDBC driver and .NET Data Provider

Prepare the Java or .NET runtime required for your application to work with the JDBC driver and the .NET Data Provider. The implementation of the encryption algorithms used to connect these applications to the database server is provided by the respective runtimes.

### Features not provided

- Windows client(32bit)

# 1.2 Operating Environment

Describes the operating environment for Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

## 1.2.1 Required Operating System

One of the operating systems shown below is required in order to use Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

- RHEL8.4 or later minor version
- RHEL9.2 or later minor version
- SLES 15 SP3 or later minor version

### Using RHEL

To use the JDBC driver, WebAdmin, and the database multiplexing feature, the following packages are required in addition to those listed in the "Required Operating System" in the Installation and Setup Guide for Server.

- java-17-openjdk

  For the RHEL versions listed below, please install the version listed or later.

  - RHEL 8.4: 17.0.5.0.8-3.el8_4 or later
  - RHEL 8.6: 17.0.5.0.8-3.el8_6 or later
  - RHEL 8.7: 17.0.5.0.8-4.el8_7 or later

# 1.3 Install

Describes the install for Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

### Advance preparation

If you use WebAdmin, you need the Java runtime to set up WebAdmin.

WebAdmin can be set up when installing Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module. Before installation, prepare the Java runtime and set the JAVA_HOME environment variable to the Java runtime installation location.

Example)

```
# export JAVA_HOME="JREInstallDir"
```

You can also be set up after installation using the WebAdminSetup command. Before setup, prepare the Java runtime and set the JAVA_HOME environment variable to the Java runtime installation location. For information about set up using the WebAdminSetup command, refer to "Setting Up WebAdmin" in the Fujitsu Enterprise Postgres Installation and Setup Guide for Server.

### Install

To use Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module, you must install the cryptographic module. Install version 3 of the cryptographic module on each machine on which you want to install the following Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module features:

- Server feature
- Pgpool-II
- Client feature

The disk space required to install the cryptographic module is 50 megabytes.

For more information on how to install, refer to the Fujitsu Enterprise Postgres Installation and Setup Guide for Server and the Fujitsu Enterprise Postgres Installation and Setup Guide for Client.

Note

You should not specify the openssl_conf and openssl_modules parameters in postgresql.conf.

# 1.4 Setup

Describes the setup for Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

### Using the database multiplexing feature

If you want to take advantage of the database multiplexing feature, you need a Java runtime.

Prepare the Java runtime and set the JAVA_HOME environment variable to where the Java runtime environment will be installed.

Example)

```
# export JAVA_HOME="JREInstallDir"
```

If Mirroring Controller connects to an instance with SSL using Red Hat build of OpenJDK, set the following in the server definition files of the primary server and standby server. For more information, refer to "Creating, Setting, and Registering the Primary Server Instance" in the Fujitsu Enterprise Postgres Cluster Operation Guide(Database Multiplexing).

- db_instance_ext_jdbc_conninfo

  If you are using Red Hat build of OpenJDK to make an SSL connection, add the following to the connection parameters:

  ```
  sslfactory=org.postgresql.ssl.DefaultJavaSSLFactory
  ```

  Use the NSS database for storing certificates and private keys. To enable the JDBC driver to access the NSS database, specify the properties you want to specify for the JVM startup options in the environment variable JAVA_TOOL_OPTIONS.

# 1.5 Application Development

Describes the application development for Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module.

### Applications using the JDBC driver

If you are using Red Hat build of OpenJDK to make an SSL connection, add the following to the connection parameters:

```
sslfactory=org.postgresql.ssl.DefaultJavaSSLFactory
```

Use the NSS database as the keystore and truststore. Specify the JVM startup options so that the JDBC driver can access the NSS database.